The integrated security system of the Senate of the Italian Republic

G. Contardi[1], F. Garzia[2] & R. Cusani[2]
[1]*Senate of Italian Republic, Italy*
[2]*Department of Information, Electronics and Telecommunication Engineering, SAPIENZA - University of Rome, Italy*

Abstract

The security of a complex site is strongly dependent on the use of integrated technological systems. Any weakness of the integrated system involves a weakness of the security of the site itself. For this reason it is necessary to design and realize highly integrated, efficient and reliable security systems. The authors illustrate the work made to design and realize the integrated security system of the Senate of the Italian Republic.
Keywords: integrated security system, control system, communication system access control system, intrusion detection system, video surveillance system.

1 Introduction

The Senate of the Republic represents one branch of the Italian Parliament (the other branch is the Chamber of Deputies). Its see is composed of 13 historical buildings located in the center of Rome in Italy.

In such a complex contest, it was necessary to design and realize a strongly integrated security system that could ensure a high interaction between the different subsystems that compose it. So the different subsystems are able to interact reciprocally in an efficient and coordinate way, showing a high degree of usability to let the security personnel to receive, in real time, the different information required to manage not only security but also emergency situations.

The system is properly divided into subsystems that are:

1) the telecommunication subsystem;
2) the video surveillance TV subsystem;
3) the access control subsystem;

WIT Transactions on the Built Environment, Vol 117, © 2011 WIT Press
www.witpress.com, ISSN 1743-3509 (on-line)
doi:10.2495/SAFE110101

4) the intrusion detection subsystem;
5) the fire detection /extinguishing subsystem;
6) the supervision and control subsystem.

In integrated security systems, the information management represents a very important factor for the functionality and efficiency of the systems themselves. In fact, due to their intrinsic nature, these systems generate a considerable information flow inside them that must be correctly addressed, coordinated, and potentially stored on temporary or permanent memory supports, to avoid overcharging or over dimensioning of communication channels and storing devices [1–8].

Figure 1: Picture of Madama palace, the main building where the Assembly of Senators is located.

The system guarantees a high degree of integration between the different subsystems, ensuring a correct and immediate control of all data and significant events for security management and control.

So the system functionalities are really superior with respect to the functionalities of single subsystems.

The system was designed and realized to reduce, as more as possible, the esthetical impact on the architecture of the Senate buildings, providing its advanced functionalities without disturbing the artistic style of the buildings from any point of view.

The system operates thanks to an advanced telecommunication subsystem, characterized by a high reliability that is capable of working in the presence of any critical condition. The telecommunication system is based upon a fixed system and a mobile system.

The designed system is characterized by a high degree of modularity and expandability so that it is possible, at any time, to add and integrate any other

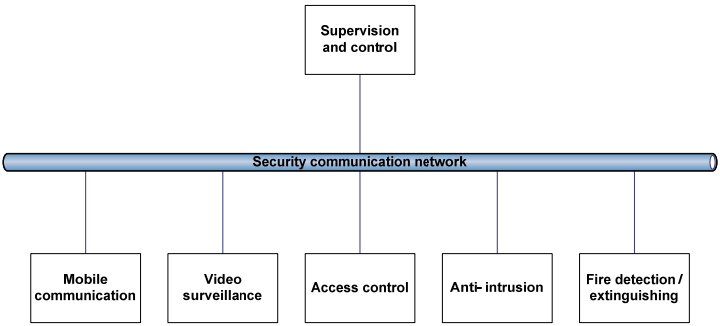

Figure 2: Scheme of the integrated security system.

subsystem, device or installation in any point of the Senate buildings, guaranteeing always the full control of any components.

Every component of the system is supplied by proper autonomous and backed-up electrical sources to be able to work even in the absence of the main electrical supply.

The system is managed by a proper main control room and some secondary workstations that allow the total control of the system in case of malfunctioning or damaging of the main control room. In this way the full control of the whole system is always ensured. The system is also endowed with disaster recovery capabilities.

A special attention was reserved, in the design of the system, to the psychological and ergonomic aspects of the operators of the control room, to avoid information overcharges that would induce stress and reduce attention level, decreasing their performances.

For this reason the information flow is processed to reduce its level in ordinary conditions and to properly increase it in emergency situations, when the operators of the control room and the other personnel must face and manage directly events that could become dangerous for people or goods.

The operators and the personnel are properly and continuously trained to make them able to analyse and to study the dangerous events, and to face them properly through functional and efficient procedures allowed by the high degree of integration of the system.

The realization of the powerful and versatile integrated security system described in this paper guarantees a high level of security services of the Italian Senate of the Republic.

2 The telecommunication subsystem

The telecommunication subsystem represents the backbone of the integrated security system (video surveillance CCTV, access control, intrusion detection, fire detection, etc.), ensuring advanced functionalities and performances.

In the following only a synthesis of the main features is illustrated.

The telecommunication subsystem is composed by two strongly integrated sub-systems: fixed infrastructure and mobile infrastructure.

The whole telecommunication subsystem is controlled by the main control room that checks the functionalities of any component of the integrated system, including the telecommunication subsystem. Any malfunctioning is immediately signalled to the operator that can activate the related procedures to guarantee the maximum functionality of the system.

The design of the telecommunication subsystem started with the analysis of security data flows that must be carried by the system.

The data flows of the integrated system are generated by video cameras, alarms, access control, voice communications, and control data.

Once known the total flow that must be carried by the telecommunication system, it has been possible to design it, dividing it into a fixed system and a mobile system. Each system has been designed according to the peculiar data flows that must be carried, following the criteria illustrated in the following.

The telecommunication subsystem is totally separated from the other telecommunication systems of the Senate, to avoid interferences that could weaken the system itself.

Further, it has been designed to guarantee a high reliability and availability using a high redundancy. In particular, it is endowed with a total autonomous electrical supply system.

The telecommunication subsystem is continuously and automatically checked so that any malfunctioning is immediately signalled and repaired. The control software examines any data flow to check any irregularity or overcharge of the system. Further, the system has been designed to guarantee a high quality of service (QoS) and class of service (CoS).

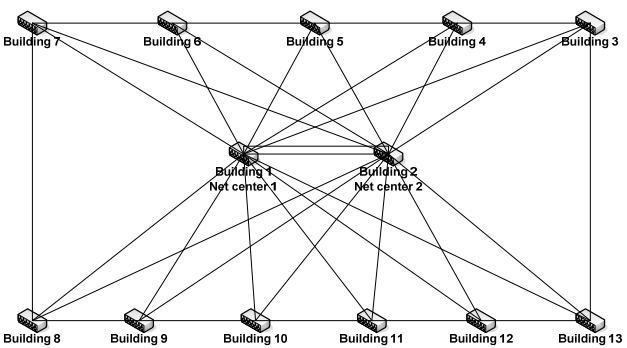

Figure 3: Network architecture.

The telecommunication network has been designed as a function of the different environments to be served and of the different protocols to be carried, to guarantee a high level of security and services.

To guarantee a high velocity of data transmission, redundant optical fibres have been used. All the connections are capable of reaching velocity of 10 Gbit/s.

The net architecture is based on dense grid connections, where two redundant centres are present, properly located into protected rooms. In this way, a damage

of a centre is immediately recovered by the other centre. Each building is endowed by a proper redundant switch connected to the main backbone by means of four links: two towards the centres and two towards the switches of adjacent buildings. The two centres of the net are connected by means of a double optical fibre. Each connection of the net follows different physical paths so that the interruption of one link (voluntary or involuntary) is immediately recovered by the other links. This kind of architecture guarantees a high level of reliability.

The fixed net infrastructure is designed and realized considering a three level hierarchic model:

1) access level;
2) distribution level;
3) core level.

The access level is represented by the most external nodes of the net, also called leaves. The main functions of the nodes are:

1) introduction of the traffic inside the network;
2) security management;
3) band management (compression, traffic-shaping, etc.);
4) congestion management (priority management mechanisms);
5) proxy services (DHCP relay, etc.).

The distribution level represents a series of policing functionalities such as service access, management and distribution of routing information and definition of the metric for the best paths choice. The main goals of this level are:

1) aggregation of the traffic coming from the nodes;
2) hiding of the network details to the core by means of IP addresses aggregation;
3) check of the dimensions of the routing tables by means of minimized core connections;
4) congestion management by means of priority control mechanism and congestion avoidance;
5) security management by means of access control list;
6) band management by means of compression and traffic-shaping mechanism.

The core level makes the following functions:

1) high velocity switching of IP traffic;
2) optimized management of net resources, bandwidth, CPU, etc.;
3) traffic distribution through paths of the same weight;
4) use of advanced techniques of QoS for policing, congestion avoidance, prioritization.

All the servers related to the management of the network are grouped in a proper server farm. It is composed by two redundant servers connected by means of a double link. These servers are connected to the two centres of the network by means of a double link so that full redundancy is always ensured.

Even if all the connections are realized in a secure way and all the devices are properly placed in secure rooms, due to the extension of the net, to increase the

security level of the system, all the links are properly ciphered by means of proper devices that allow the creation of Virtual Private Lans.

A series of Virtual LANs (VLAN) are defined for every switch of building and for the two centres of the network. These VLANs are used for the connection of the different devices of the system and for the connection of the switches of building with the other components of the net infrastructure.

The mobile communication subsystem is designed to allow a prompt diffusion of security information and a rapid response of personnel involved in any emergency situation. It is strongly integrated with the other components of the telecommunication subsystem.

The mobile subsystem is based on TETRA standard, a technology expressly developed in EU for security and safety communications.

Due to the variety of problems involved, a collective access radio system has been designed and realized. It is capable of satisfying all the security communication needs of the Senate. The mobile system is composed by a series of base stations (BSs) (such as ordinary GSM or UMTS mobile communication system) connected to a central unit that manages and controls the service of radio units of the users.

The mobile communication system is composed by a control centre, called master site (MS) and from a variable number of base stations (BSs) positioned on the territory.

Every BS can support 4 radio channels per transmitted carrier and can operate simultaneously on different carriers.

The MS is located in a protected zone inside the main control room. The main operator console is connected directly to the MS where it is possible to operate directly on the mobile system, programming the database and the user's profiles.

The MS is connected directly to the PBX to interface with the internal and external telephone lines.

The radio units are characterized by reduced dimensions and weight and by controllable emitted powers, always ensuring the better communication quality between the radio units and the nearest BS. It also includes a GPS receiver for the positioning services and a Bluetooth interface to connect to an external terminal, where it is possible to receive and control alarms and signalling (data, picture or video) coming from the supervision system.

The number and the positions of the BSs have been calculated by means of a proper and complex simulation and study of electromagnetic propagation (using Genetic Algorithms optimization): it ensures a full coverage of the buildings and of the related interiors, respecting the severe environmental electromagnetic emissions limitations imposed by the Italian law.

The frequencies used are between the interval 380–400 MHz that ensure a greater propagation inside the buildings and the narrow streets around them, guaranteeing an optimal coverage of the area.

In a collective access radio system the frequency are dynamically assigned to the users, according to their needs, allowing an efficient and dynamic management of the system.

The mobile system allows the interconnection with the internal and the external telephone net, guaranteeing a high level of connectivity.

Every used radio link can be divided in 4 different channels, that are used singularly or together as a function of the necessary transmission band.

The mobile subsystem checks continuously the coding/decoding quality of the voice, allowing an optimal communication service even in the presence of noises.

Thanks to the GPS receivers integrated inside the mobile terminals, it is possible to see on proper maps, in the control room, the position of users, greatly improving the quality of security and emergency services and procedures.

3 The video surveillance subsystem

The video surveillance subsystem (VSS) is designed to allow the operators to control any zone of the buildings and to reconstruct, in a second time, any kind of event thanks to the high storing capabilities of the subsystem. It also integrates the alarms coming from the other subsystems, providing a visual access to the area of the signalled events.

The integration with the other subsystems is realized by means of:

1) a supervision system, that represents the central element for the management of the whole security system;
2) direct integration, obtained through the direct connection of the different components of other subsystems.

The VSS uses the communication services offered by the security network described above to transmit images, both in real time and recorded, to the interested operators. The stored images access is properly restricted to comply with Italian privacy laws.

The VSS is capable of individuating any intrusion attempts through the external perimeters of the buildings. For this reason it is necessary to transmit, in real time, all the images necessary to evaluate the events or to send them to proper automatic devices that analyse the scenes and generate an alarm to the operator only in the dangerous situations.

Images acquisition is made through an optimal visualization of the controlled areas, using both wide angle and narrow angle camera objectives, according to the characteristic of the zones.

The VSS has been designed and realized to guarantee high standard of efficiency, quality, scalability, opening, operative flexibility, reliability and security, according to the respect of privacy imposed by Italian privacy laws.

The VSS is based on a mixed analogical/digital architecture. All the cameras are analogical, to guarantee a high quality of images to be analysed, locally, by proper analysis devices. The images are locally converted in digital format, by proper local video server, to be sent towards the control room and towards the distributed consoles which need those images, using a TCP/IP protocol. The VSS is composed by the following main components:

1) cameras: two different kinds of cameras are used: fixed, to control the entrances of the buildings; dome, to control the external areas.

2) video servers: they convert the analogical signal coming from cameras into a digital signal to be sent through the dedicated security network;
3) images analyzers: they analyze the images coming from the cameras, through advanced techniques and algorithms to reveal, automatically, critical situations. The related alarms are sent to the related operators through the telecommunication network;
4) control and visualization consoles: the consoles are present in the following points: main control room; entrance gatehouses of the palaces;
5) recording system: it stores all the images coming from the cameras through the network and it is located in the main control room. The access to the images archive is properly protected to comply with the Italian privacy laws;
6) telecommunication network: it represents the backbone of the whole security system and it has already been described before. It allows the communication between all the components of the video surveillance subsystem.

The VSS is composed by the following logical elements:

1) field devices (cameras);
2) digitalization devices;
3) image analysis devices;
4) recording devices;
5) management devices;
6) operator interfaces.

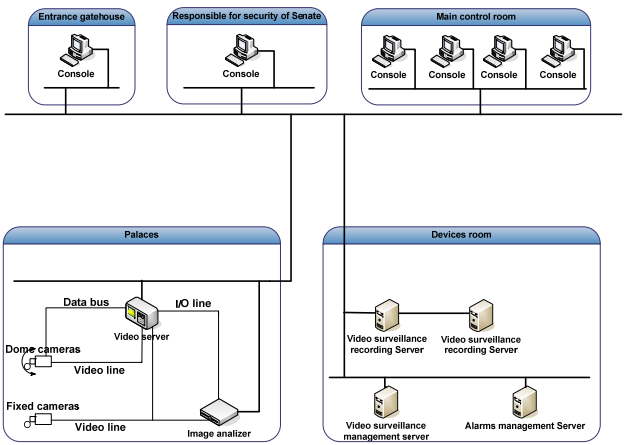

Figure 4: Physical architecture of the video surveillance subsystem.

4 The access control subsystem

The access control subsystem (ACS) controls all the entrances of the buildings and the technological installation rooms.

It is characterized by a high modularity so that it is possible to add in any moments further entrances without any problems.

The ACS uses hands-free radiofrequency badges together with biometric face recognition and all the event are properly visualized and recorded by means of the video surveillance subsystem. Locally it is also present a display that shows the face of the entering person together with the image recorded into the database for an immediate visual recognition and control to be made by the entrance security personnel.

The ACS is based on a distributed architecture with central database and regional databases. In this way, in case of temporary loss of the network, the subsystem is capable of working without any problems, updating the central database when the communication is restored.

The ACS is composed by the following main components: central server; biometric central server; regional servers; entrance controllers; entrance consoles.

The central server stores the user profiles, the installations configuration, the history of alarms and events. It duplicates this information on the regional servers.

The biometric server stores the face pictures of users, importing the related information and profile from the central server. It duplicates this information on the regional servers.

The regional servers store all the information related to the users and all the history of alarms and events that have verified in the controlled entrance. It communicates with the central server and with the biometric central server to keep updated the central database.

The entrance controllers work as interface between the regional servers and the badge readers, sensors and electrical lockers of the automatic entrances.

The entrance consoles are located close to the entrances and are used by the security personnel. They allows to: visualize the transits and the face of entering people; manage the alarms; manage the entrances; check the state of every entrance devices (sensors, actuators, badge readers, etc.); configure the local ACS components.

Every operation made by the operators is properly recorded into the ACS and it is available to be controlled in a second time.

The radiofrequency badge readers comply with all the international laws concerning human exposure to electromagnetic fields and are characterized by a reduced emission level.

The badges are composed by three sections: radiofrequency; magnetic strips; microchip, to be used with all the internal operative services of the Senate.

In case of malfunctioning of one modality (radiofrequency badge or face recognition) the entrances can be enabled to work in a single modality instead of double modality to guarantee anyway the access to the people. In this way the security personnel is aided by the real image of the person compared, on the display, with the image stored into the database.

Proper consoles are located into the office dedicated to the generation and print of badges for face enrolment and storage into the database.

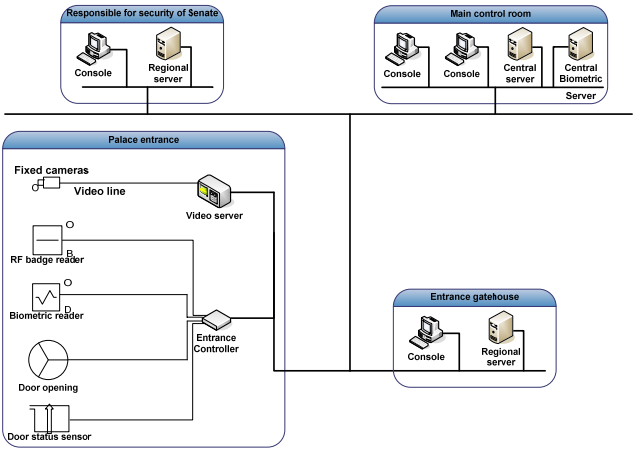

Figure 5: Physical architecture of the access control subsystem.

5 The intrusion detection subsystem

The anti-intrusion subsystem (AIS) is dedicated to the perimeter control of the buildings and to the acquisition of internal alarms activated by means of proper buttons. It uses proper input/ output (I/O) modules to read the field sensors information and to send them, through the network, to the consoles of the control rooms. It allows: concentration of the alarms towards the dedicated consoles; control of the field devices to inform in real time the central system of eventual anomalies and malfunctioning to request proper repairing procedures; interfacing with the other subsystems, in particular the video surveillance, to activate joint procedures in case of alarm (such as activation of the nearest cameras to view directly the alarmed zones).

The AIS, like the other subsystems, is totally autonomous and self- consistent so that it is capable of working even in the absence of control by the supervision subsystem.

The field sensors are represented by: perimeter barriers on the terraces; magnetic contacts on door and windows; anti-aggression button; mobile radiofrequency alarm button devices.

The AIS is characterized by a high modularity so that it is possible to add in any point further I/O modules, thanks to the capillary presence of the security network in any building, and further field sensors.

The I/O modules can connect to the field sensor by means of direct connection or by means of serial bus connection. They can be programmed to interface with any kind of device and communication protocol.

All the alarms and events are displayed on the consoles of the control rooms.

6 The supervision and control subsystem

The supervision and control subsystem (SCS) is the integrating element of the different subsystems (even if these last one are also connected at a lower lever in some cases), offering superior functionalities with respect to the functionalities offered by the separated subsystems.

It allows an optimization of the management and control procedures, reporting all the signalling and alarms on the consoles of the control room.

The SCS uses an open software platform extremely flexible and programmable so that it is very easy to be used and to be expanded to add new components in a second time.

The SCS uses the dedicated security network to exchange information with the different subsystems to control them even if they are totally autonomous from the SCS, being able to operate even in the absence of coordination.

The advanced functionalities of the SCS are available on the consoles of the control room even if any console can be added in any place of the Senate for particular and momentary needs thanks to the capillarity diffusion of the security network.

All the information is shown on proper maps, to allow a clear and immediate view and management of the events through appropriate software buttons present on the maps themselves.

All the alarms, the signalling and the operator actions are stored into the historical database of the SCS.

The SCS is characterized by: integration with other subsystems; autonomy from the other subsystems; expandability; scalability; operative flexibility; reliability; high security level.

It can control: single sensors and cameras; whole installations; any other element and device in the field.

It is composed by: central redundant servers; consoles; security telecommunications network.

The logical architecture of the SCS allows us to divide it into two functional modules: control module and operator module.

The control module is constituted by three different sub-modules: data acquisition; data processing; client management.

The data acquisition sub-module takes care of interfacing with other subsystems, managing all the problems related to the connection with other plants and related to the coding/decoding of messages (communication protocols). It mainly adapts the data received from the field sensors and installations in the standard format useful for the control module.

The data processing sub-module is the core of the subsystem and it takes care of controlling the data, generating alarms and actuating the actions associated to the alarms. It can work under the supervision of the operator or automatically, according to pre-defined procedures. The automatic actions can be divided in: storing of the state variation into the historical database; alarm generation and notification to the interested operator consoles; storing of the alarms in the historical database; activation, without operator action, of a pre-defined

command after a proper signalling; reproduction of an audio file, on the interested operator consoles, to signal a particular event; automatic opening of a video windows, on the interested operator consoles, to show the image related to a particular event; automatic opening of a synoptic map, on the interested operator consoles, to show a particular event.

The client management sub-module manages the information exchange with the operators, answering to the interface requests and sending it all the data.

The operator module represents the element of SCS that interacts with the operators.

The operator module is constituted by two different sub-modules: supervision and control; configuration and management.

The supervision and control subsystem takes care of interfacing with the operators to allow the full control of the subsystems.

The configuration and management sub-module allows the specialized personnel to configure and manage the whole system. It is controllable through proper dedicated console, whose access is properly protected.

Both the sub-modules communicate with the control module, in particular with the client sub-module, to: receive the events signaling coming from the controlled subsystems and send them the action to be executed; send the configuration information.

7 Conclusions

The security management in complex contests such as the Italian Senate of the Republic needs a detailed risk analysis and a correct study, design and realization of an efficient telecommunication subsystem that is capable of integrating the different security subsystems, thanks to the aid of a supervision and control subsystem, ensuring the maximum reciprocal interaction of the different subsystems involved.

In this way it has been possible to realize a powerful and versatile integrated security system that guarantees a high level of security services of the Italian Senate of the Republic.

References

[1] Waltz, E., “Information Warfare – Principles and operations”, Artech House Publisher, Boston (USA), 1998.
[2] Denning, D. E., “Information Warfare and Security”, Addison-Wesley, Boston (USA), 1999.
[3] Nichols, R.K. & Lekkas, P.C., “Wireless Security: Models, Threats, and Solutions“, McGraw-Hill”, New York (USA), 2002.
[4] Garzia, F., “The integrated safety/security system of the Accademia Nazionale dei Lincei at Corsini Palace in Rome”, Proc. of International Conference on Integrating Historic Preservation with Security, Fire Protection, Life Safety and Building Management Systems, Rome (Italy), pp.77-99, 2003.

[5] Garzia, F. and Veca, G. M., "Integrated security systems for hazard prevention, management and control in the Italian high speed train line", *Risk Analysis III*, WIT Press, Southampton (UK), pp.287-293, 2002.
[6] Antonucci, E., Garzia, and F. & Veca, G.M., "The automatic vehicles access control system of the historical centre of Rome", *Sustainable City II*, WIT Press, Southampton (UK), pp.853-861, 2002.
[7] Garzia, F., Sammarco, E., and Cusani, R., "Integrated access control system for ports", *Safety & Security Engineering III*, WIT Press, Southampton (UK), pp.313-323, 2009.
[8] Garzia, F. Sammarco, E., Cusani, R. "The integrated security system of the Vatican City State", Int. J. of Safety & Security Eng., WIT Press, Vol.1, No.1, pp.1-17, 2011.